AFRL-IF-RS-TR-2002-175
Final Technical Report
August 2002

JOINT C4ISR ARCHITECTURE PLANNING/ANALYSIS SYSTEM (JCAPS)

Northrop Grumman Information Technology

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

AIR FORCE RESEARCH LABORATORY
INFORMATION DIRECTORATE
ROME RESEARCH SITE
ROME, NEW YORK

This report has been reviewed by the Air Force Research Laboratory, Information Directorate, Public Affairs Office (IFOIPA) and is releasable to the National Technical Information Service (NTIS). At NTIS it will be releasable to the general public, including foreign nations.

AFRL-IF-RS-TR-2002-175 has been reviewed and is approved for publication

APPROVED: 

RICHARD J. LORETO
Project Engineer

FOR THE DIRECTOR: 

JOSEPH CAMERA, Chief
Information & Intelligence Exploitation Division
Information Directorate

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	JULY 2002	Final May 97 – Dec 01

4. TITLE AND SUBTITLE
JOINT C4ISR ARCHITECTURE PLANNING/ANALYSIS SYSTEM (JCAPS)

5. FUNDING NUMBERS
C - F30602-96-C-0353/
F30602-99-D-0264/T4
PE - 31335F
PR - R528/R528
TA - 00/QT
WU - 02/04

6. AUTHOR(S)
Bill Wostbrock

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Northrop Grumman Information Technology
Defense Mission Systems Division
12005 Sunrise Valley Drive
Reston Virginia 20191

8. PERFORMING ORGANIZATION REPORT NUMBER
N/A

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Air Force Research Laboratory/IFEB
32 Brooks Road
Rome New York 13441-4114

10. SPONSORING / MONITORING AGENCY REPORT NUMBER
AFRL-IF-RS-TR-2002-175

11. SUPPLEMENTARY NOTES
AFRL Project Engineer: Richard J. Loreto/(315) 330-3793/ Richard.Loreto@rl.af.mil

12a. DISTRIBUTION / AVAILABILITY STATEMENT
APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

12b. DISTRIBUTION CODE

13. ABSTRACT ***(Maximum 200 Words)***

The contractor satisfactorily completed all tasks under both efforts, providing the technology and technical expertise in the development of the Joint C4ISR Architecture Planning/Analysis System (JCAPS) Database Tool. JCAPS is an automated software application designed to support the interoperable, integrated, and cost-effective business practices and capabilities for warfighters and acquirers across DOD particularly with respect to information technology. Using JCAPS, warfighters can plan, execute and manage C4ISR assets in support of military operations. The final report summaries the effort.

There are two contract numbers listed in block 5 above. In FY 99, there was a cut in funding associated with the JCAPS effort, contract F30602-96-C-0353. It became apparent that based on the funding cut and the way in which we received funds and the type of vehicle that was in place, the best way to support our customer was to convert the contract vehicle to an IDIQ contract. The prime contractor remained the same, there was no break in service and in Sep 99, F30602-96-C-0353 was converted to F30602-99-D-0264.

14. SUBJECT TERMS
JCAPS, Database, C4ISR, C4ISR Database Tool, Architecture

15. NUMBER OF PAGES
16

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	UL

Table of Contents

List of Figures

List of Tables

1.0 JCAPS OVERVIEW

The Joint Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) Architecture Planning/Analysis System (JCAPS) is an automated software application designed to support the interoperable, integrated, and cost-effective business practices and capabilities for warfighters and acquirers across DoD, particularly with respect to information technology. It provides uniform methods for describing information systems and their performance in context with mission and functional effectiveness.

Using JCAPS, war-fighters can plan, execute and manage C4ISR assets in support of military operations. The system helps Joint Force Commanders synchronize the C4ISR actions in support of air, land, sea, space, and special operations forces. It has the flexibility to be used in supporting a vast range of operations: from actual combat to humanitarian assistance.

1.1 BACKGROUND

The JCAPS integration effort is preceded by the Integrated Command, Control, Communications, Computers, and Intelligence (C4I) Architecture Requirements Information System (ICARIS) effort.

The *C4ISR Architecture Framework, Version 2.0*, as part of a larger DoD initiative for improved interoperability and Joint Force integration, provides common guidance and methodology for building C4ISR architectures. Each architecture development is made up of one or more of three architectural views: the Operational Architecture View, the Systems Architecture View, and the Technical Architecture View. Combined, these three views are used to define, compare, and visualize operational concepts and requirements; guide systems development and rapid allocation of resources; provide alternative solutions in support of contingency operations; and support Joint and Combined Forces interoperability.

In support of the *C4ISR Architecture Framework, Version 2.0* that defines DoD architectures, JCAPS is designed to be a common system for identifying, comparing, contrasting, and integrating C4ISR architectures by the CINCs/Services/Agencies (C/S/As). JCAPS has been identified as the

direction that automated applications should take to ensure that architecture planners can analyze, integrate, and migrate from existing to objective architectures.

1.2 SYSTEM ARCHITECTURE

JCAPS employs a three-tiered client/server architecture in both software and system design. Every major feature of JCAPS is packaged in the following ways: as a software component supporting the presentation tier, a software component supporting the server tier or a software component supporting the data storage tier. JCAPS operates on a Windows NT platform, and supports the exchange of data between war-planning scenarios and a centralized Oracle database. Table lists the functionality unique to each tier.

Table 1. JCAPS Three-Tiered Functionality

PRESENTATION TIER
• ***Interface with the server tier to create, review, modify, query, report, and display data. No direct access to the database server is available.***
• ***All data edited is buffered and passed on to the server tier.***
SERVER TIER
• ***Responsible for retrieving all required data to pass on to the presentation tier.***
• ***Responsible for retrieving all required data from the presentation tier to pass on to the data storage tier.***
• ***Contains all the algorithms for the manipulation and processing of data that is application specific; i.e., beyond the realm of what can be performed in a stored procedure.***
• ***Responsible for the multi-user data locking and unlocking mechanism.***
DATA STORAGE TIER
• ***The repository for stored procedures in support of the presentation tier and server tier.***
• ***Stored procedures are responsible for all business rules and data access, including insert, update, and delete. This enforces data integrity and the security access required within JCAPS.***
• ***Provides role-based dynamic views for independent read-only access by non-JCAPS front-end tools.***

The three-tiered system architecture design for JCAPS allows JCAPS to operate as a stand-alone application, on a local area network (LAN), or on a wide area network (WAN). This design permits the easy configuration of JCAPS for any of these environments without requiring separate versions of the software.

1.3 CURRENT FUNCTIONALITY

The JCAPS Prototype Version 2.1.1 Patch 1 provides for the creation, maintenance and reporting of Architectures as depicted in the *C4ISR Architecture Framework, Version 2.0*, along with the individual elements and six of the Operational and System products. JCAPS also provides one additional product that blends the Operational and System views together. See Section 7, *Working with Products*, in the *JCAPS User Manual (UM),* for details on current products.

1.4 CONFIGURATION

The JCAPS Prototype Version 2.1.1 Patch 1 can be used with the presentation tier, server tier, and data storage tier installed on the same platform (the stand-alone configuration). It can also be used with the three tiers on separate platforms. Given the heavy transaction processing between the JCAPS Server and the Database, the preferred installation is to co-locate both of these components on the same platform and install the presentation tier on separate workstations, as required. Refer to the *JCAPS System and Database Administrator Guide (SAG)* for details on installation requirements and procedures.

1.5 SECURITY ASSESSMENT

1.5.1 SECURITY REQUIREMENTS

JCAPS will be used in the System-High Mode of Operation and is expected to be classified as a C2 system. As such, JCAPS, in conjunction with the operating system and the database, is designed to provide the following

security policy-enforcing features or mechanisms: Identification and Authentication, Audit, Object Reuse, and Discretionary Access Control.

Each user with direct or indirect access to the system must possess a valid personnel clearance for all of the information on the system (i.e., formal access approval and signed non-disclosure agreements for all of the information stored and/or processed on the system; and a valid need-to-know for some, but not necessarily all, of the information contained in the system).

1.5.2 INITIAL LIMITATIONS

The JCAPS Prototype Version 2.1.1 provides discretionary access controls by which the user can control access to his or her data

JCAPS defines and controls access between named users and data groups in JCAPS Prototype Version 2.1.1. The enforcement mechanism allows users to specify and control sharing of those data groups by named individuals, or defined groups of individuals, or by both, and provides controls to limit propagation of access rights. The discretionary access control mechanism, either by explicit user action or by default, protects data groups from unauthorized access. These access controls are capable of including or excluding access to the granularity of a single user. Only authorized users can assign data-group access-permissions to users not already possessing access permission.

The system administrator defines users and user groups consisting of one or more users. Then, the system administrator and individual users create data groups to which individual user(s) and/or group(s) are assigned permissions.

1.5.3 RESIDUAL RISKS

Only partial Defense Information Infrastructure (DII) Common Operating Environment (COE) compliance checking has been accomplished. We can not assure that the JCAPS installation or program use will not adversely affect other programs without complete DII COE compliance checking. Thus, there is some risk that the JCAPS Prototype Version 2.1.1 will not operate satisfactorily in an environment with other programs loaded.

1.5.4 CONDITIONS OF USE

The JCAPS Prototype Version 2.1.1 may be used under an Interim Authority to Operate (IATO) provided by the JCAPS Program Management Office (PMO). This authorizes your site to install JCAPS Prototype Version 2.1.1 release in support of prototype operational testing in accordance with the constraints listed below:

- Installation of the JCAPS software must be approved by the site Information Systems Security Officer (ISSO) and the Designated Approving Authority (DAA).

- At the discretion of the site, workstations used for the Prototype Version 2.1.1 can be loaded with software other than that software directly needed to operate JCAPS (i.e., Windows NT, Oracle, Excel, and JCAPS). If it is determined the configuration will not support JCAPS prototype operations, Logicon will identify any necessary changes or constraints directly with the site.

- Workstations will be configured to a high level of security as defined by the Microsoft abstract Securing Windows NT Installation.

- Prototype release operational test Sites will ensure the functional separation between SIPRNET and any other networks (e.g., NIPRNET) when JCAPS is installed on a LAN with access to the SIPRNET, including use of the web interface portion of JCAPS on SIPRNET.

- Only persons involved in the prototype release operational testing will be given access to JCAPS.

- The JCAPS software will not be used beyond the duration of the prototype operational testing without prior approval of the JCAPS Program Manager and the site ISSO. The prototype testing period is extended to 1 August 2001.

- The JCAPS PMO will provide classified data no higher than SECRET collateral for use during the prototype testing. JCAPS will be used by sites to process no higher than SECRET collateral data during the prototype operational testing, since the prototype has not been subjected to the full security accreditation process. Sites that desire to operate at a higher

security level may do so on standalone machines only and must locally meet all cognizant security requirements for their site.

- The site must provide the Defense Information Systems Agency (DISA) Information Assurance Program Management Office (IPMO) with a "Consent to Monitoring" authorization. The site must submit appropriate documentation to the cognizant security authority(s) for operations higher than SECRET collateral.

- The site must provide an Interim Authority to Operate (IATO) to DISA (IPMO) for approval before the site can use the JCAPS system on the SIPRNET. The site must submit appropriate documentation to the cognizant security authority(s) for operations higher than SECRET collateral.

- The site must update its SIPRNET configuration.

Prototype test participants will be asked to provide feedback to the JCAPS PMO.

1.6 FUTURE DIRECTIONS

The JCAPS application will ensure a coordinated and consistent approach for management of local and shared C4ISR architectures and data within the DoD. JCAPS is a product evolving from user-driven requirements and goals of the Global Command and Control System (GCCS) and DII COE, with the ultimate ambition of integrating and improving the interoperability of C4ISR systems via shared architectures.

JCAPS will include a suite of tools and connectivity to a data repository that holds a core set of common and shared Department of Defense (DoD) C4ISR architecture data as well as private data at local repositories. JCAPS will provide the user with an interactive, distributed, and networked C4ISR architecture planning tool in the GCCS within the DII COE.

JCAPS will combine several powerful technological resources, resulting in a broad range of potential users. These resources will include visual diagramming tools, the latest in Geographic Information System (GIS) mapping technology and the ability to exchange data with a vast repository of military data across a global network. Because of the number of mission-

planning capabilities and the vastness of the centralized database, the limitations of JCAPS are harder to identify, with its potential uses and users seemingly without limitation. It can be used as a basic architecture-diagramming tool to outline possible real-life scenarios. It can also tap into the centralized database in order to depict real life resources and the logistical details of operations.

1.7 PLANNED FUNCTIONALITY

The software components within each tier are designed to provide specific functionality, as illustrated in Table 0-1. Note that many of these functions are not currently available (as denoted by *) and will be phased in during the life cycle of JCAPS.

Table 0-1. JCAPS Components within the Three Tiers Making Up JCAPS

PRESENTATION TIER	
Architecture View	**Architecture Templates**
Architecture Wizards*	**Architecture Objects**
SERVER TIER	
Diagramming Engine	**Analytical Computation***
Web Access*	**Statistics and Metrics***
Data Access	**On-Line Help***
Report Engine*	**Control Center**
GIS/Mapping Engine*	
DATA STORAGE TIER	
Data Migration and Import/Export*	**Performance Monitoring**
Backup /Recovery	**Database Management**

1.8 NETWORK ENVIRONMENT

The potential LAN and WAN implementations, as well as the future use of a trusted security guard for multi-level secure operations, are depicted in Figure 0-1. The three tiers of the JCAPS architecture are shown, consisting of multiple JCAPS clients in the presentation tier, two JCAPS server-tier servers (Sensitive Compartmented Information (SCI) and SECRET), and two JCAPS database servers (SCI and SECRET) in the data storage tier. The two JCAPS server-tier servers in this configuration contain both the application server and the optional web server. For those JCAPS users who just want simple dynamic reports from the JCAPS database and basic access to the JCAPS database, the optional web server allows for cost-effective access.

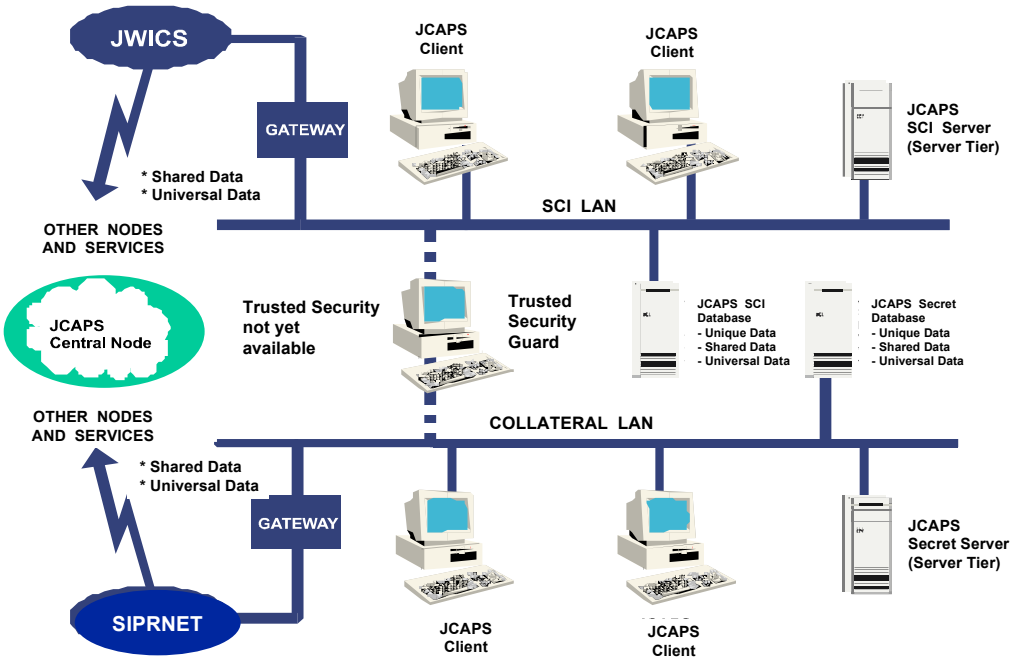

Figure 0-1. JCAPS in a LAN/WAN Configuration

In stand-alone mode, all components belonging to the three tiers are simply installed on the same computer, excluding the JCAPS web server. The JCAPS web server is not needed because native functionality already exists.

For collaborative efforts, data sharing, and connectivity to the JCAPS Central Node, JCAPS will connect to other nodes and services over the SECRET IP Router Network (SIPRNET) and in the future to the Joint Worldwide Intelligence Communications System (JWICS). This will permit JCAPS to share data through replication, and to share functionality with JCAPS components at other nodes. In this manner and with the addition of other data exchange formats, JCAPS will lend itself to potential interaction with such tools as the Model Reference Technology (MRT), the Joint Mission Area (JMA) Analysis Tool, the Levels of Information Systems Interoperability (LISI), the Ptech FrameWork C4ISR Model, and the Virtual Joint Technical Architecture (VJTA).

1.9 DATA SHARING

Data sharing between JCAPS nodes will take two forms: automated replication of data that is applicable to all sites and manually selected push/pull sharing of site-selected information. In keeping with the shared data environment (SHADE)-type data classification, data that is applicable to all sites is referred to as universal data and data selected for sharing from one site to another is referred to as shared data. Shared data will primarily consist of architectures.

1.10 UNIVERSAL DATA

Universal (replicated) data will be made available in the future to all sites from the JCAPS Central Node through automatic Oracle replication processes. When the owner of a universal data set makes new data available to the JCAPS Central Node it will be entered into the system for replication. The data will disseminate to all sites on the network and be loaded into each site's database automatically. No site intervention is required in the receipt of universal data and the site's unique data is unaffected. Sites that are temporarily off the network will automatically update as soon as they return to the net.

1.11 SHARED DATA

Shared (replicated) data will also be processed through the JCAPS Central Node, with that node acting as the go between for the data. A site may manually select the other sites with which they wish to share data. The data to be shared will be pushed to the JCAPS Central Node by a series of Oracle stored procedures and triggers. The process then will notify the sites receiving the shared data that the data is available for their download. When a site is ready to receive data that has been shared, it will initiate another set of stored procedures to pull the data from the site's database and make it available to the site's users. Complete instructions on how to share an architecture with a specific site will be included in Section 8.4. Private data (i.e. non-replicated data) will not be shared.

1.12 COLLABORATIVE PLANNING

Sites will also be able to work on architectures and architecture products in a collaborative mode. Using the same network used for data replication and sharing, users at one site will be able to log on to the application server at a remote site and work on the remote site's architectures and products as if they were remote site users. To operate in this mode it will be necessary for the site's users to be granted log on and access privileges at the remote site.

1.13 STAND-ALONE OPERATIONS

Users who are using stand-alone JCAPS implementations will be able to obtain universal and shared data from the JCAPS Central Node by dialing into the JCAPS Central Node. Once connected, the stand-alone JCAPS will appear on the network just like any other JCAPS site. If the stand-alone JCAPS is unable to dial in, universal and shared data may be updated through the use of SHADE-type data segments. The SHADE-type data segments will contain the data that will represent each subject area of the JCAPS physical data model. The advantage of the SHADE segments is that they allow transfer of information to JCAPS implementations that are not on a network.

1.14 DATA MAINTENANCE

Certain types of data used in architectures are normally maintained by selected cognizant organizations within DoD. To prevent the introduction or incorporation of incorrect information, JCAPS would capture such universal information directly from the cognizant authorities. Examples of data normally maintained by cognizant organizations include the following:

- The Joint Technical Architecture (JTA)
- Unit Identification Codes (UIC)
- The Universal Joint Task List (UJTL)
- Equipment specifications

Technical architecture information is one of the three types of architecture views likely to be under the control of cognizant organizations. JCAPS users are likely to access, but not change, technical information. Thus, most JCAPS technical architecture information will be made accessible through the SIPRNET.

2.0 Conclusion

The JCAPS system provides continuing coverage for the DoD to meet the directive set forth by the ASD/C3I in 1995. The JCAPS serves as the first effort into a global architecturing tool and has been installed at most major CINCs, Service Headquarters and agencies. After the reduction of funding in the second year of the effort, the JCAPS has achieved a significant number of architecturing and system enhancements and to this day, the JCAPS is the only architecturing system that provides the security and multiple user features in an architecturing system that could provide for the original goal of a global shared architecture database. The project continues with enhancements to the system such as the GIG and CADM compliance efforts.

Northrop Grumman Information Technologies - Point of Contact:

Bill Wostbrock
Tel: 813-286-7335
Fax: 813-282-1821
Email: wwostbrock@mail.northgrum.com
200 South Hoover Boulevard
Mariner Square 201, Suite 170
Tampa, FL 33609